HOUSE OF LORDS

SESSION 1997–98
5th REPORT

OU/L

SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY

DIGITAL IMAGES AS EVIDENCE

REPORT

Ordered to be printed 3 February 1998

LONDON: THE STATIONERY OFFICE
£7.80

HL Paper 64

WELLCOME
LIBRARY
P
8517
22501831079

HOUSE OF LORDS

SESSION 1997–98
5th REPORT

SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY

DIGITAL IMAGES AS EVIDENCE

REPORT

INFORMATION SERVICE 0
XUA 17 APR 1998 06
HoulL
Wellcome Centre for Medical Science
12430

Digital television
Evidence (Law)

Ordered to be printed 3 February 1998

LONDON: THE STATIONERY OFFICE
£7.80

HL Paper 64

CONTENTS

	Paragraph	*Page*
CHAPTER 1 INTRODUCTION	1.1	5
A Picture is Worth a Thousand Words	1.1	5
Traffic control	1.4	6
Document imaging	1.6	7
Overt surveillance using CCTV	1.7	7
Covert surveillance using CCTV	1.9	7
Acknowledgements	1.10	8
CHAPTER 2 BACKGROUND	2.1	9
"So what is special about Digital Images?"	2.1	9
Altering a digital image	2.5	10
The need for caution	2.11	11
But are these concerns real?	2.12	11
The current law on the use of images as evidence	2.14	12
Special requirements for admissibility	2.15	12
CHAPTER 3 DIGITAL IMAGES	3.1	15
Proving the accuracy and assessing the weight of evidence	3.2	15
Some implications for handling digital images	3.7	16
Requiring the original image to be produced to the court	3.10	19
Excluding the use of digital images as evidence unless specific requirements are met	3.15	20
Identification in the Criminal Court	3.22	21
The current need for greater certainty	3.28	22
Maintaining confidence in the accuracy of the image	3.29	23
CHAPTER 4 CIVIL LIBERTY IMPLICATIONS	4.1	25
City Centre Surveillance	4.3	25
Benefits and Concerns	4.4	25
Current Controls over the use of CCTV	4.9	26
Control of public CCTV Images	4.10	26
Surveillance Coverage	4.12	28
Control of CCTV in spaces to which the public has free access	4.13	28
The Data Protection Act	4.15	29
Data matching	4.18	29
Conclusion	4.22	31
CHAPTER 5 SUMMARY AND RECOMMENDATIONS	5.1	32
APPENDIX 1: Membership of Sub-Committee II		34
APPENDIX 2: Call for Evidence		35
APPENDIX 3: List of Witnesses		36
APPENDIX 4: Acronyms		37

REFERENCES IN THE TEXT ARE AS FOLLOWS:

(Q)	refers to a Question in oral evidence
(p)	refers to a page in HL Paper 64-I of this Session

FIFTH REPORT

3 February 1998

By the Select Committee appointed to consider Science and Technology.

ORDERED TO REPORT

DIGITAL IMAGES AS EVIDENCE

CHAPTER 1 INTRODUCTION

A Picture is Worth a Thousand Words

1.1 The tabloid at the supermarket check-out may have another "Elvis is Alive" story with a picture of him holding the last month's issue: inside there might be a story about a World War II Lancaster bomber landing on the moon, with photographs to prove it. But by and large people do not believe these photographs however real they look, and it is doubtful if the authors expect them to. So why should people doubt the photographs in a broadsheet of the Chancellor of the Exchequer holding up his red box on Budget Day in front of No. 11 (*The Guardian* 3 July 1997)[1]? Even those who approach what is written with a reasonable degree of scepticism have a general presumption that a photograph is what it purports to be. Further, if a jury in a criminal case is shown by the prosecution a clear and unambiguous photograph of the defendant caught in the act, in the absence of any other evidence, will the members regard it with just the same degree of scepticism as they had for the picture of the Lancaster on the moon? And should they?

1.2 Questions such as these led the Committee to embark on its study of the use of digital images as evidence (see Box 1 for background information on images). What initially seemed likely to be a short enquiry into an apparently straightforward and well contained topic was found to be far less constrained. The ubiquity of digital technology meant the subject broadened from images, typically photographs, to closed circuit television (CCTV) on the one hand and databanks on the other. Digital technology has a pervasive influence on many apparently unrelated aspects of society, which was one of the reasons why in our previous report "The Information Society: Agenda for Action in the UK"[2] we recommended that the Government take a holistic approach by setting up an Information Society Task Force to identify the barriers to the development of the Information Society in the United Kingdom and to recommend appropriate remedies.

1.3 Although there is a common technological link between the many different issues raised by digital imaging, their apparent diversity makes it difficult to draw a common theme for this report. For example, the discussion of CCTV and city centre surveillance would not be complete without reference to the issues raised for individual privacy. But while an examination of the principles behind the moves towards a law of privacy is clearly not part of the remit we have set ourselves, an analysis of the implications for the individual created by the application of new technology, and hence the willingness of the public to accept it, is. Similarly when considering the implications of documentary data we found ourselves looking at the Data Protection Act. Again,

---

[1] Picture editors at *The Guardian* used Photoshop software and Apple Macintosh computers to remove an individual standing behind the Chancellor on the steps of No. 11 Downing Street on Budget Day, in order to 'improve' the image.

[2] 5th Report, 1995–96, *The Information Society: Agenda for Action in the UK* (HL Paper 77).

Box 1: What is an image? Some definitions

Analogue images

The traditional image captured by photography is an **analogue image**. The images are recorded as a variation in some physical property, for example frequency, amplitude, or activation state of a photochemical emulsion (of colour dyes and silver halides, for example, as a transparency or a negative). This varies with the brightness, colour and contrast of the scene being recorded.

Digital images

A digital image is a numerical representation recorded simply as a series of binary digits (bits): either one or zero with no values in between. The image is captured by being focused onto an electronic sensor (a charge coupled device, CCD) which is made up of individual light-sensitive elements called **pixels** (picture elements). These act as switches modifying an electrical current on or off and the information is processed by a computer. Images may be either moving or still, the data can be stored on a variety of media (eg compact disc, computer hard disk, or digital tape), and the image may be displayed either on an electronic display (computer monitor, TV screen or computer projection) or as a hard-copy print.

Image resolution

The quality of a digital image depends on the number of sensor pixels and the size of the image as it is displayed. High resolution digital cameras on general sale at the moment have 'million pixel' sensors 1,152 x 864 pixels, (eg the Kodak DC210 for around £650) which will produce a standard five inch by three and three quarter inch photo with a resolution of 115 dots per inch. Compared to an analogue print of the same size, this sort of resolution is very poor but is suitable for displaying on a computer screen. Higher resolution sensors are available and it is likely that they will become more widely available in the near future. Much higher resolution is also available from computer scanners which can be used to digitise paper documents and analogue photographs. Epson, for example, sell a 2,400 dots per inch scanner for just over £500. If linked to their 1,440 dots per inch colour laser printer (for around £200), this can produce a photo-quality hard copy.

with proposed legislation underway it is not our intent to comment on the Data Protection Act[3]. Nonetheless, digital imaging technology has broad implications here for the way we run our society which we cannot ignore. We have taken the initial focus of our study—the digital image, typically in the form of a photograph—and looked at the two adjacent topics: moving images (videos and CCTV) and images of text, either written or as 'pictures' that exist only as data on a computer. All forms of evidence can raise questions of authenticity: digital images are not unique in this respect. For example, questions of forgery arise with more conventional technology. But digital technology raises its own sort of issues and these are the subject of this Report. First we describe some of the ways in which imaging technologies are being used today.

Traffic control

1.4 Most roadside traffic enforcement cameras monitoring speeding offences and red light violations record the image of the offending vehicle onto photographic film which has to be stored at the roadside. This presents a series of problems: the film needs to be kept secure, the film needs to be changed often, the number of incidents recorded is limited by the film capacity, each film needs to be collected and taken for processing, and then has to be analysed before a 'Notice of Intention to Prosecute' is issued. If a digital camera is used instead, or the image from a traditional camera can be converted into digital data, then there are many advantages: incidents can be recorded almost indefinitely as these data are down-loaded to a computer, the data store for many cameras can be at one central and secure location (eg in a police station) rather than by the road, processing is done by computer and, if number plate recognition software is used, the registered owner of the vehicle can be identified immediately. The ultimate in automation is for the computer then to print a Notice of Intention to Prosecute and send it out to the offender without human intervention— although we emphasise that this is not current practice.

---

[3] The Government introduced the new Data Protection Bill on 16 January 1998 as this report was being finalised.

1.5 Home Office requirements for digital enforcement systems specify the camera resolution to be used (approximately 1000 x 1500 pixels), image compression standards for when the image is transmitted to the computer, transmission encryption protocols and standards for storing and archiving images. An authentication code is also required to be added to the image. The level of security during transmission of the image data is similar to the encryption used by banks to secure the electronic transmission of data which occurs when a cash machine (automatic teller) is used.

Document imaging

1.6 The Abbey National told us that they had revolutionised their document management system by using optical scanners linked to computers with character recognition software. Original paper versions of mortgage applications, for example, were now scanned electronically to produce a digital image; this was stored in computer memory from which it could be retrieved and viewed at any time. Alterations could not be made to this digital copy, but annotations could be added in the form of overlays to the image (QQ 334–8). The Abbey National told us that the digitisation of documents reduced the risk of loss, damage or alteration, inherent in paper-based processing. The scanning stage was seen as the critical step and this was under secure management; the risk of files being deleted or substituted after this initial processing was controlled through the implementation of an audit trail which recorded all accesses.

Overt surveillance using CCTV

1.7 A surveillance system inside a large shop or a town centre will usually consist of a number of cameras with pan, tilt and zoom controls which feed live colour pictures back to monitors in a control room. The camera output is also recorded and this is usually on to high quality videotape. To extend the period between tape changes, the recordings are often only made at two frames per second. CCTV systems depend to a large extent on the quality of the camera and the lens used. For example a system which might be used in a shopping centre would have a 96x optical and digital zoom, autofocus, 370 degree per second pan and 120 degree per second tilt (to move the camera rapidly between pre-set positions), and an in-built image processing computer.

1.8 Some cameras also have infra red capabilities for surveillance during the hours of darkness, and motion detection sensors to warn operators of unusual activity and start recording more detailed images. For example, the City of London Police use motion detectors to alert operators when a vehicle has transgressed an exit point of the traffic control zone in the City. Other camera features available include: bullet-proof and explosion-proof casings; automatic defence mechanisms, to ensure that if a camera comes under attack it is filmed by its neighbours; systems which automatically switch from full colour to black and white to maximise image resolution if the lighting level drops; and directional microphones.

Covert surveillance using CCTV

1.9 The quality of image available from digital CCTV cameras is still poor compared to the high resolution available with analogue cameras, but one area where they have a great advantage is in covert surveillance. Tiny digital cameras a few centimetres square can now be bought which offer 300,000 pixel resolution and low-light sensitivity. At least one company in the United Kingdom is also offering these cameras disguised in anything from mirrors and pictures to smoke detectors and clocks.

Acknowledgements

1.10 The membership of our Committee is listed in Appendix 1 and the Call for Evidence we issued is set out in Appendix 2. The Enquiry was based on the assistance of a wide range of individuals and organisations who responded to the Call for Evidence: these are listed in Appendix 3. We are most grateful to them all for their time and effort. We also wish to express our thanks to those whom we visited, who made presentations or provided briefing: in particular the City of London Police together with the Symonds Group Ltd; the Greater Manchester Police; the Forensic Science Service, and Epsom and Ewell Borough Council. We have been greatly assisted by our Special Adviser, Mr Chris Reed, of Queen Mary and Westfield College. We very much appreciated the help of all those who have contributed to this Enquiry.

CHAPTER 2 BACKGROUND

"So what is special about Digital Images?"

2.1 A key element of digital technology is the ease with which perfect copies can be made (see Box 2). Attempts to copy a conventional analogue audio tape produce an inferior copy but a digital copy of a digital compact disc (CD) is an identical replica. This is one of the great benefits of digital technology. However it can also create commercial difficulties for the manufacturer trying to prevent the production of counterfeit goods, for example. Other key features of digital technology are the ease with which data can be changed and the ease with which data can be matched with information from other databases (see Chapter 4). As one of our witnesses said: "with recent increases in computing power at affordable prices and improvements in imaging hardware, image manipulation has become far more accessible" (p 150). The Chartered Institute of Arbitrators also cautioned that even colour laser photocopiers commonly featured editing facilities, so that tampering with an image is no longer the preserve of computer science (p 156). This is both a great advantage and a severe problem of the technology.

2.2 If presented with an 'original' digital image and a copy, perfect in every respect, in the absence of any other information it is impossible to distinguish which one was produced first. In many circumstances this might not matter, but if the data are transferred to a computer, modified in some way and then returned to an identical storage device to the one they were recorded on (eg to an identical looking CD which is passed off as the 'original'), it might matter. It would matter greatly if the item described as an 'original' were a photograph of a defendant apparently involved in a criminal activity. Equally, the Crown Prosecution Service expressed concern that the technology could give defendants "the ability to construct an alibi that is convincing ... using home video equipment to manipulate an image" (p 168).

2.3 Here we find that there is some confusion over what can be described as the original when considering digital images, in particular between the technical and legal definitions (see Box 2). We prefer the following definition in relation to digital images: the original is the data first recorded in memory. Thus any printed or displayed image created from these data is a copy. Consequently digital recording technology provides no original that could be produced in evidence. All that is available for use as evidence is a copy of the first, probably temporary, recording in memory, and this will be admissible as evidence. Its weight as evidence will depend on proper authentication and other matters.

2.4 In relation to a digital camera, for example, it is probable that the original would be the digital file representing the image which is stored on a memory chip, or series of chips, at the moment that the image is captured. That digital file will immediately be copied to some other form of storage and the memory chip will be overwritten with the next image[4]. This does not represent a problem under the law of England and Wales because if the original of a document no longer exists, copies or even copies of copies are admissible in evidence[5] and it is irrelevant that the original was destroyed by the person seeking to produce the copy as evidence[6]. Nor is it a problem in Scotland because although the general rule[7] that copies of documents are admissible whether or not the originals still exist does not apply to visual images[8], copies of a document which no

---

[4] US law provides that printouts of data stored in a computer are 'originals' under Fed. R. Evid. 1001(3), and even if not original are normally admissible as duplicates unless there is some doubt as to their authenticity (rule 1003). The records are always admissible if the originals have been destroyed (rule 1004).

[5] There is a misconception, presumably derived from the old best evidence rule which is now largely superseded, which stated that where the original of a document existed it must be produced before the courts in preference to a copy. *R v. Wayte* (1983) 76 Cr. App Rep 110. "It is now well-established that any application of the best evidence rule is confined to cases in which it can be shown that the party has the original and could produce it but does not" (*per* Beldam J. at p 176). See also Civil Evidence Act 1995 s. 8(2).

[6] Unless, of course, there is evidence that the original was destroyed to suppress evidential weaknesses.

[7] Paragraph 1 of Schedule 8 to the Criminal Procedure (Scotland) Act 1995.

[8] Paragraph 8 of Schedule 8 to the Criminal Procedure (Scotland) Act 1995.

Box 2: What is an original?

An analogue image always has an original to which it relates in either negative or positive form (ie the negatives from which photographic prints are made, transparencies or the magnetic recording on a video tape). Copies can be made from the original and normally there will be little difference between them, but as further copies are made from these copies then the image quality is likely to deteriorate.

For a digital image the 'original' consists of the data recorded in memory, from which the image can be generated. Because the recorded image is represented as a finite set of numbers, exact copies may be made, and images made from these copies. Each stage of copying is precise and there is no loss of image quality between generations. Thus it becomes impossible to say which is a first generation image: the implication is that any digital image can be thought of as being 'the original' even if it is produced from a copied set of data, unless it is tagged in some way to identify it as the first image made (see Box 4 on authentication).

An original for the purposes of the law of evidence is usually the first manifestation of a document in final form. However, where there are multiple possibilities (eg where a fax is sent, both sender and receiver have 'original' copies) the original for some purposes is that version of a document which was intended by its maker to be legally effective.

Because of the possibility of different interpretation of 'original' in law, we have adopted the definition of paragraph 2.3.

longer exists are admissible under the best evidence rule[9]. The fact that a document is a copy goes to its weight as evidence, not its admissibility. It will therefore be necessary for the user to be able to give evidence of the procedures used for generating, processing and storing digital images, so as to be able to prove that the image produced to the court is an accurate copy of the original[10]. But in general, provided it would not prejudice a fair trial, the court is likely to admit the evidence and the judge will direct the jury on the weight they should consider attaching to it.

Altering a digital image

2.5 Because a digital image is just a visual representation of ones and zeros in computer memory it may be altered, deleted or copied at will in the same way as any other computer data. An image may be altered in much the same way as a word processor can be used to change the text of a document: the final text when displayed need give no clue as to how many words or paragraphs have been changed from the first version, nor who changed them and when (or why). A variety of software packages are available which allow one to sharpen and enhance the image, change colours, contrast and brightness, copy and move around segments of the image, and import image segments from other photographs to make a seamless collage. The sequence of a 'movie' can also be altered or reversed to show events in non-chronological order. As discussed in Box 2, the ultimate modified image may be indistinguishable from the first version in terms of quality or the apparent representation of reality.

---

[9] *Lord Advocate's Reference No. 1 of 1992* 1992 SLT 1010 at p 1018 J-K.

[10] This evidence will not be necessary in civil proceedings if the authenticity of the image is admitted during discovery under RSC Ord. 27 r. 4(1), which provides that where lists of documents are exchanged a document which is asserted on the list to be a copy is presumed to be a true copy unless its authenticity is specifically disputed by the other party. If the document is disputed, however oral evidence as to authenticity will be required. In criminal proceedings, it will always be necessary to be able to produce some founding testimony as to the source and authenticity of the image, otherwise the courts may refuse to admit the evidence.

2.6 The potential for making subtle, but significant, alterations to an image gives most cause for concern as such changes may be highly convincing and almost impossible to spot. For example, software is available which can be used to add or subtract shadows and ensure that the sun angle on an object (perhaps a person) imported into a base image is congruent with the rest of the scene. Timing mechanisms on electronic devices often do not keep accurate time (and they are often set incorrectly to start with, Q 104) and visual cues from a scene that might corroborate timings (eg a clock face) are easy to alter or obscure.

2.7 In the course of criminal proceedings it may be necessary to use computer techniques to enhance an image, making the subject clearer (eg by removing signal noise) or isolating the subject from a cluttered background to make identification easier. If the image is to be used for evidential purposes, the question that might be asked is, what represents justifiable enhancement? Does this differ from manipulation which might have, or be perceived to have, malicious intent, and where can the distinction be drawn?

2.8 Changing the contrast or colour balance of a computer monitor may be considered visual 'enhancement' and is no different from what might be done to an analogue image. However, any alterations which affect the image data, no matter how innocuous, should be treated with caution. Sharpening the outline of an object is a standard option on image-processing software which usually involves changing the contrast at the edge of the image (eg black pixels against grey pixels may become black against white). After sharpening, the object is easier to see, but the image data have been changed.

2.9 Some modifications are made routinely for image processing, for example de-skewing a page as a document is scanned electronically. The process is automatic, uses a set algorithm to make simple adjustments and if agreed limits are placed on the scope of the operation then this perhaps should be accepted as a justifiable modification. Cleaning-up unwanted signals that arise from outside interference might also be acceptable, although it would be better to ensure that the imaging system is immune from such signals in the first place.

2.10 If human judgement is involved and the process is more complicated, then the resulting image is of questionable evidential value. For example, improving the clarity of a face in a still from a grainy security video will depend on the software and equipment used, the assumptions made about that face (and this in turn will depend on the bias of the operator), and the composition of any comparative data set used as a reference. Value judgements will be made during the process. There is no clear distinction between acceptable 'enhancement' and unacceptable 'manipulation'. Any changes have to be considered on their merits.

The need for caution

2.11 With modern processing and tele-communication techniques even an image that purports to be analogue may have had a 'digital past'. For example, it is possible that an image stored digitally may have been generated with a standard analogue camera, the signal or picture may be converted into digital format for transmission and then converted back to analogue again to be displayed. Thus, in many circumstances, it can be difficult to make a distinction between what is and what is not a digital image (Abbey National Q 353). The ease with which images, when in digital format, can be copied and modified suggests that caution must be exercised when *any* image is being used as evidence: all images, both analogue and digital might be suspect.

But are these concerns real?

2.12 We took much evidence as to the power of image modification technology (eg Mr Sommer, Mr Davies and Mr Smith, and witnesses from IBM), saw it for ourselves thanks to the assistance of the Forensic Science Service and the Greater Manchester Police, and heard about its widespread availability, low cost and the difficulty of detecting modifications (eg Mr Sommer, Q 115). We concluded that before the advent of digital technology it might have been a time consuming and costly exercise to produce a modified image in which it was difficult to detect tampering, but with the present widespread availability of digital technology it could now be a low cost operation to produce an image in which the modifications would be undetectable[11]. The existence of a technology that can be used to modify images in this way need in itself be of no great concern; even the widespread availability of the technology at low cost might not cause concern. But an apparent lack of understanding of the implications of both these facts should cause concern and warrants further study. The public and all those in the legal profession (Mr Smith Q 84) should be made more aware of the technology, what it can do, and what its limitations are. It was suggested that criminal convictions that were dependent on evidence captured by digital cameras could be at risk if defence lawyers began to realise how vulnerable such images are to manipulation. This means that when presented with an image the observer should have no more, and no less, faith in it than if the information had been text on a sheet of paper of questionable provenance.

2.13 However, we also heard that digital images presented opportunities: Mr Marcus, Senior Legal Counsel for IBM, held the view that digital images presented "positive evidentiary opportunities ... for the identification of content owners (owners of copyright) and of unauthorised modifications in ways which are not available to traditional analogue technologies" (Q 261). For example, images could be time-stamped or given other authenticating marks.

The current law on the use of images as evidence

2.14 Although there is no legislation which expressly covers digital images used as evidence, nor any reported cases in which the fact that an image was collected in digital form was at issue (Crown Prosecution Service p 167) there is a substantial body of the law of evidence which deals with the problems arising from technological recordings. This body of law will equally apply to digital images. Indeed, witnesses including the Senior Counsel from IBM (Q 263) and solicitors from Bird & Bird (Q 78) regarded the differences between digital images and other evidence as being one of "degree rather than of fundamental kind" (Q 78).

Special requirements for admissibility

2.15 The rules of evidence of common law jurisdictions normally exclude from evidence certain types of document. The most unreliable kind of evidence, under these rules, is 'hearsay', which is not admissible as evidence unless it falls within one of the numerous exceptions to the rule. By contrast, information captured by a recording device, with no human intervention, is not normally hearsay and can be admitted in evidence. Video and image recordings are not therefore excluded as hearsay.

2.16 In civil litigation, there are no prior requirements which must be met before a document (which would include a digital image) can be admitted in evidence. Section 1 of the Civil Evidence Act 1995 abolishes the hearsay rule for civil proceedings, and Section 8 provides that where a statement in a document is admissible, it may be proved by producing a copy of the document (even if the original is still in existence) and that the number of removes between a copy and the original is irrelevant (ie it may be an n^th^ generation copy). Furthermore, under Section 9, documents which form part of the records of a business (defined very widely) are automatically admissible and the absence of an entry in those records can be proved by an appropriately signed certificate[12].

---

[11] If the technology exists then it is inevitable that it will be used: for example, the Newport Beach Police Department in Anaheim, California, have recently been testing Adobe Photoshop image processing software to isolate and give greater clarity to suspects in CCTV images.

[12] Note that not all business documents are 'records'. *H v. Schering Chemicals* (1983) 1 All ER 849, the leading case on the meaning of 'record', indicates that a document, irrespective of its form, will only be a record if (a) it effects a transaction or is a contemporaneous compilation of information derived from primary sources which is intended to serve as a record of events; and (b) it is a comprehensive compilation, rather than a selection of source information. If a document is not a comprehensive record of what has occurred, or, even if comprehensive, was not intended to serve as a primary source of information on that matter, it will not be a record. Thus the majority of computer records will fall under s.8 rather than the more favourable provisions of s. 9. A certificate signed by an officer of the business is required under s. 9(2) so as to demonstrate that the document forms part of its records.

2.17 In criminal cases the position is a little different, as the House of Lords has decided[13] that the provisions of Section 69 of the Police and Criminal Evidence Act 1984 (see Box 3) apply to all computer records, whether they are hearsay or not. This means that in criminal cases, any use of a digital image as evidence must be accompanied by the certificate required under Section 69. This certificate, given by a person responsible for the computer system in question, must state that either the computer system was at all times operating properly, or that any defect in its operation was not such as to affect the accuracy of the record.

Box 3: Police and Criminal Evidence Act 1984 (PACE)

Section 69 of PACE refers to the admissibility of evidence from a computer, and requires assurances about whether the equipment was being used properly and was functioning normally at the time. The implication of Section 69 is that any party relying on computer evidence has to provide oral or written certification of the reliability of the computer, or for each computer if a number have been involved.

Section 69 Evidence from computer records

(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown:
  (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
  (b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and
  (c) that any relevant conditions specified in rules of court under subsection (2) below are satisfied.

(2) Provision may be made by rules of court requiring that in any proceedings where it is desired to give a statement in evidence by virtue of this section such information concerning the statement as may be required by the rules shall be provided in such form and at such time as may be required.

2.18 The Law Commission has recently recommended the repeal of Section 69 of PACE because it "serves no useful purpose". The Law Commission said that it was impractical to certify all the intricacies of computer operation and experience showed that most computer error was either easy to detect immediately or had resulted from human error in data entry rather than from malfunction. With the repeal of Section 69, a presumption of proper functioning would be applied to computers (Evidence in Criminal Proceedings: Hearsay and Related Topics, LAW COM No. 245, June 1997).

2.19 As new technology (and in particular information technology) finds a place outside the research laboratory, its reliability and accuracy is established through use and public acceptance grows through familiarity (or indifference). Debate over the use of the technology moves on from whether the hardware and software are reliable to how the technology might be used to greatest effect, hence the move by the Law Commission. If the proposal of the Law Commission is accepted, legal challenge to new technology may now be reoriented to establishing authenticity and suitable weight for the evidence which it generates.

2.20 The underlying problem that remains is the potential for image tampering: how to be sure that an image has not been unfairly modified and what, if any, image processing in the name of 'enhancement' is justified. The Home Office already gives 'type approval' for systems where the only evidence of a crime is an image taken by an enforcement camera (eg speeding and bus lane violations), but the general concept of a 'self authenticating image' and how it might be used in a court of law is still something which needs to be evaluated.

---

[13] *R v. Shepherd* (1993) 1 All ER 225.

2.21 The courts always have discretion to exclude evidence which has doubtful probative value. A prosecutor or party to litigation will always need to be prepared to offer further evidence about the source of a digital image and the processing and storage it has undergone since it was first recorded. It has been held that the person adducing a recording as evidence must describe its provenance and history, so as to satisfy the judge that there is a *prima facie* case that the evidence is authentic[14].

---

[14] *R v. Robson & Harris* (1972) 1 WLR 651, a case concerning an audio recording.

CHAPTER 3 DIGITAL IMAGES

3.1 We decided that our study should be centred on photographic-like images and was bounded on one side by documents and on the other by closed circuit television (CCTV) and video. We have discussed the background to current law in Chapter 2. In this chapter we examine some of the issues which go towards proving the accuracy of an image and assessing its weight. We look also at some suggestions for establishing requirements for the use of images in court, any need to provide information or warnings to those who use them, and we make recommendations.

Proving the accuracy and assessing the weight of evidence

3.2 Authentication is the process of convincing the court that a document (which would include a digital image) is what it purports to be: of proving the origin of the image and that it has not subsequently been altered (or, where alteration has occurred, proving the nature of the alteration). Even though an image has been authenticated, however, the court will still need to determine its weight as evidence, its probative value. This depends both on the degree of authentication and the extent to which the image provides evidence of the fact in question. For example:

- An image which appeared to show the defendant in the act of committing a crime, but for which there was no explanation as to its origin or other authentication, would have a very low probative value[15]. Conversely, an identical image originating from a police CCTV camera for which a detailed audit trail could be produced would have a much higher probative value. The greater degree of authentication of the second image increases its weight as evidence.

- However, if the image were so blurred as to be unrecognisable, or if the court were not convinced that any enhancement processes which purported to reveal the identity of the defendant were reliable, it would give little or no weight to the image as evidence, irrespective of how well it was authenticated. A factor which would clearly increase an image's weight as evidence is compliance with relevant standards, such as the BSI standard for image storage in computer memory of the "Write Once Read Many Times" (WORM) type[16] (See Box 4).

3.3 The fact that a document is a copy may reduce its weight as evidence, unless there is sufficient authentication evidence to convince the court that it is an accurate copy. This authentication evidence would normally be in the form of an audit trail connecting the original image with the computer record which is to be adduced in evidence and recording what has occurred to that record in the interim (eg Mr Sommer, Q 115). As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features of the system or the record (see Box 4). Oral evidence will concentrate largely on the management and operational procedures applied to the computer record. Ideally these should be assessed by the lawyer in advance to ensure that a satisfactory audit trail can be produced. Circumstantial evidence will cover a wide variety of matters, including the record's consistency with other documents which make up a linked transaction. Technical evidence might come from system logs, particularly if they are designed specifically with this end in mind, or through embedded features of the record itself such as watermarks and digital signatures; although these are only of any real use for authentication if the encryption key is outside the control of the person adducing the evidence[17].

---

[15] And it would probably not be admitted as evidence under the rule in *R v. Robson & Harris* (1972) 1 WLR 651.

[16] The British Standards Institution Code of Practice for the Legal Admissibility of Information on Electronic Document Management Systems (DISC PD 0008, February 1996) sets out procedures and documentation required for the audit of systems producing documents or other images that may be used as evidence in a court of law. The Standard focuses on procedures rather than technology and thus continues to be relevant. It does, however, specify optical storage (CD ROM) as the standard WORM device for storing data as this was the only technology available at the time (BSI QQ 206–207, and ST/97/DI/38). The BSI told us that this would be updated and that a new code was being written to cover authentication (Q 211).

3.4 A number of cases where the authentication of computer records was at issue have come before the courts, and where there has been no suggestion that the records might have been altered deliberately or accidentally, the authentication requirements have been met by evidence from those responsible for operating the computer system in question[18]. In *R v. Spiby*[19] the English Court of Appeal was prepared to presume that a computer was recording evidence accurately when its operator (a hotel manager) testified that he was unaware of any problems in operation, in the absence of any evidence from the defendant that there was any question of malfunction, and in *R v. Shepherd*[20] a store manager's testimony was held by the House of Lords to be sufficient for the same reasons.

3.5 This evidence will not be necessary in civil proceedings if the authenticity of the image is admitted during discovery under Rules of the Supreme Court, Order 27 rule 4(1) which provides that where lists of documents are exchanged a document which is asserted on the list to be a copy is presumed to be a true copy unless its authenticity is specifically disputed by the other party. If the document is disputed, however, oral evidence as to authenticity will be required.

3.6 Of considerable interest to us was that no defence teams in the United Kingdom had, as yet, ever requested an audit trail be produced in any case where video images were being used by the prosecution (eg Liberty Q 4). This may change as defendants and their lawyers become more familiar with the technology.

Some implications for handling digital images

3.7 Modern offices employ sophisticated data processing technology for document handling. If a form is sent off to a building society, bank or insurance company, it may be imaged and thereafter handled by networked computers. This is done for reasons of business efficiency (eg to speed up processing and to reduce the need for file storage space in the office). Any document can be available instantaneously throughout the organisation and it does not get lost (eg Abbey National system Q 320). When text is examined, be it on hammered vellum or a computer screen, certain fundamentals have to be in place. Put simply, it has to be verified that it is what it purports to be. Traditionally, verification has been through the use of an authenticating mark or signature. In the digital age, something rather more complex is often required: for documents this can be a digital signature which incorporates encryption, making the signature unique to the specific document and its originator; and for other images an electronic watermark may be used (various authenticating technologies are discussed in Box 4).

3.8 Some witnesses, including the Association of Chief Police Officers in Scotland (p 154) and the Crown Prosecution Service (p 165) were in favour of images incorporating some form of watermark or other authentication (added at the time of image capture) to increase their utility in

---

[17] However, encryption for security reasons might also have an authentication function if it could be used to show that the number of persons with power to alter the record was limited, and that those persons had no motive or opportunity for alteration. These points are, of course, only relevant if the image's status as an authentic copy of the original is questioned.

[18] Authenticity will be presumed if:

(a) the user can produce a human witness to testify that the system was operating properly at the relevant time; and
(b) the other party to the litigation is unable to adduce evidence to counter this presumption.

Because the image will necessarily be a copy there is thus a need to prove that each is an authentic copy of the image that was first captured. The obvious way of so doing is to give oral evidence about the procedures for storing documents and the controls which are in place as part of the system. Failure to give such evidence in relation to a copy will render the copy inadmissible under English law. *Kajala v Noble* (1982) 75 Cr App Rep 149.

[19] *R v. Spiby* (1990) 91 Cr. App. R 186.

[20] *R v. Shepherd* (1993) 1 All ER 225.

Box 4: Image authentication

The digital processing of images, the potential for image modification and the problem of defining what is an original make it difficult to establish with ease that an image is authentic. This is a critical step if an image is to be used as evidence. There are two elements to establish authenticity: to have an 'audit trail' which records everything that happens to the image from capture to its presentation in court; and/or to have a technological solution which brands or 'watermarks' the image at the time of capture and can subsequently show it is authentic.

Audit trail

Audit trail methodology is already used with other forms of evidence to ensure that it has been treated fairly, that any processing it has undergone (eg in a forensic laboratory) is well documented, that its location is always known and that all those who have had contact with it have the necessary authorisation. This is all common sense and similar controls would be expected for digital images. If an image is generated by a system dedicated to the enforcement of law then it is possible to start the audit trail at the moment of image capture, but if an image is from elsewhere, for example a photograph from a member of the public or even a CCTV video from a private surveillance system operator, then the audit trail may only start once the image is presented (or seized) by which time it may have already been modified. The courts deal with such problems with all evidence, but the ease with which digital images can be modified, the availability of the technology and the skills to do this, and the low awareness of the potential problem, should raise extra concerns.

WORM memory

Most CCTV systems and enforcement cameras make a recording onto video tape in either real time or a limited number of frames per second basis. The video recorders and tapes can be kept in physically secured areas with limited access to reduce the possibility of tampering. Further security can be achieved if a second recording is also made onto a **WORM** ('write once read many times') memory device at the same time. A WORM memory is something to which computer data can be written only once. An indelible recording is made which cannot be overwritten with other data. The data can, however, be read as many times as wished. The most easily recognisable WORM memory is a CD or CD ROM: a plastic disc coated in reflective material into which pits have been etched physically. The laser in a CD player will read the information stored in this etching, but cannot change or delete the etchings.

Recording on to a WORM will provide an image for comparative purposes which cannot be altered. However, the expense of such systems, the extra storage capacity required, the non-reusable nature of the WORM storage media, and the need to ensure that only certain people get access to the secure copy (eg the police when an investigation is started) means that such systems are probably inappropriate for wider use.

In itself, a recording on a WORM is also no guarantee that an image is free of modifications: the data could be copied to a computer, altered, and then copied back to a second identical device leaving no evidence of impropriety unless there was some other way of distinguishing the first WORM from the second.

Watermarks

Watermarks provide an extra level of security to an image in addition to an audit trail if they are added at source as the image is being captured by the camera. With a conventional image the watermark (eg an identifying code or logo) would need to be visible in the scene and may thus obscure other vital information. In a digital image it is possible to hide the watermark within the image data with a form of encryption: although the watermark can be present in all parts of theimage (down to pixel scale), the image looks normal and the watermark can be viewed only with the appropriate decryption key. It would also be possible to **encrypt** the whole image so that it is meaningless to anyone viewing it without the appropriate equipment and decryption key.

Two types of invisible watermark are envisaged and are being developed by companies including CRL IBM, NEC and others (see IBM evidence for detailed description of watermarking technology). The first (a **permanent** watermark or **'tattoo'**) will help copyright owners monitor the use of their material. The watermark is hidden within the image and will remain with the image (or image segment) if it is copied, modified or otherwise processed (ie the watermark is almost impossible to destroy or remove from the image no matter what is done to it). For evidential use this would allow copyrighted materials to be identified, and it might also be useful for identifying the source of images which have undergone significant modification. The second type of watermark is the **fragile watermark** which is destroyed by any processing or modification attempt other than just viewing the image. This could have significant potential for authenticating images used in evidence: an image which should have a watermark but does not, or has a damaged one, would have low evidential value without other corroboration.

The main limitation of all watermarks is that ideally they should be applied by the camera and thus the camera manufacturers have to install software which will do this. Only if watermarking becomes the norm for cameras where images might be used for evidential purposes, or if there is overwhelming demand from customers, are manufacturers likely to adopt such technology. There are also problems with the export/import and use of certain levels of encryption technology which might be used to generate watermarks.

Digital signature

Digital signatures can be used for authenticating messages and documents sent electronically and, equally, could be adapted for authenticating images. The American Bar Association (Digital Signature Guidelines: *http://www.abanet.org/scitech/ec/isc*) describes digital signatures as using public key cryptography and a 'hash function' derived from the message itself. The hash function is an algorithm created from enough of the message data to ensure that it could only be created from those data. The message and the hash function are then encrypted with the sender's private encryption key to make a digital signature which is unique. The receiver decodes the message with a related version of the encryption key previously given to the intended recipient by the sender (or held by a trusted third party). The message is verified by computing the hash function again and comparing it with the original.

evidence. However many other witnesses (eg the Home Office and Forensic Science Service (p 128), Mr Castell (p 160), Justice (p 3) and the Chartered Institute of Arbitrators (p 156) held the view that all such technologies were fallible and were thus of limited use. Even if complex watermarking or high levels of encryption are used then, eventually, someone may crack the code and either remove a digital signature or re-instate a fragile watermark after making modifications to the image. Authenticating technologies must therefore keep ahead of possible abusers in order for them to remain of value.

3.9 The costs both in the initial capital for the equipment and running costs of these modern office systems are substantial. We heard from witnesses (eg Abbey National QQ 321–325) of unease over the acceptability of digital technology in the courts, their concern that a large and growing data processing investment may be at risk from litigation and that large legal costs might be incurred before the matter was resolved. There was also an inability to take full advantage of the technology by, for example, destroying original paper copies[21] until doubts were resolved; for example Abbey National said it had "no experience of using digitised images as evidence in any court of law and will not be content to rely on them until their legal status has been confirmed" (Abbey National p 109). We therefore looked further at the difficulties, real and imagined, over the use of digital images in court.

Requiring the original image to be produced to the court

3.10 One possibility for overcoming the problems of digital images would be to require the production of the original as evidence before the courts (Liberty p 11). However, as discussed in Chapter 2, a fully electronic process provides no physical original. Provided the necessary verification and authentication measures are in place, we think this suggestion is misplaced. Nonetheless the very suggestion gives rise to the apparent need to keep original pieces of paper when documents are imaged for subsequent electronic handling.

3.11 One of the key implications of the growing availability of digitally captured and stored images (whether of documents or pictures) is that the erstwhile reliance on paper and photographic originals (or authenticated copies of these originals) is no longer always going to be feasible for use in court. For example the National Automated Fingerprint Identification System has no original paper source to retrieve as 'best evidence' in a court of law (p 126). Provided that verification and authentication measures of digital material are in place, paper originals will rarely be necessary. Yet the evidence we have received suggests that there may still be some reluctance to come to terms with this development. **We recommend that the Government encourage the appropriate legal bodies to draw greater attention to this change and to widen public awareness that paper originals are rarely necessary.**

3.12 A modification of the suggestion that only originals should be admissible as evidence is that where an image has been enhanced or otherwise altered intentionally, any use of the modified copy as evidence should be accompanied by the unaltered image (Justice Q 26, Liberty p 11). The founding testimony which explains the source of the image would be expected to disclose whether modification had taken place (eg in the forensic laboratory) and other parties would be entitled to copies of the unaltered image. But what assurances are there that the image was not altered before being used as evidence? There is a danger that legal advisers do not understand the possible effects of enhancement or they do not recognise that other evidence for the provenance of the image may be required, or both. These dangers would be compounded when there are insufficient resources to secure expert legal and technical advice.

3.13 In this context proposals were made to us for changes to the law. For example, that the rules for civil and criminal procedures should be amended so as to require any person putting forward a digital image as evidence to disclose to the other side an authenticated copy of the image prior to processing and details of that process.

---

[21] There may be a significant cost saving in storing electronically rather than on paper: a 70 per cent reduction in cost was suggested to us (BSI, Q 219). However one must also be aware of the need to store not only the data, but also the machines capable of reading and interpreting that data.

3.14 In this, as in the other areas, we were not convinced that rewriting the law in an attempt to keep pace with technological change was a sensible approach. The certainty we have is that technology will continue to change. No less certain is that the rate of change will increase. Thus, we agree with the Data Protection Registrar (Q 222) that attempting to extend legislation by introducing specific technological caveats to take account of the latest technology is unlikely ever to be a successful approach.

Excluding the use of digital images as evidence unless specific requirements are met

3.15 Some witnesses (eg Liberty p 4, Mr Sommer, p 45) suggested that digital images should only be admitted as evidence if the technology used to capture those images incorporated some form of authentication technology such as watermarking or a digital signature. Indeed, Mr Sommer went as far as saying that "without authentication digital images are worthless".

3.16 We have outlined earlier the existing requirements for admissibility of evidence (see Chapter 2). The arguments against specifying new criteria which must be met before evidence can be admitted are:-

- it would be very difficult to specify the nature of the authentication technology in such a way that it would not quickly become outdated as the technology advances.
- it would take an appreciable time for manufacturers of digital image technology to incorporate such measures, and even longer for such technology to become widely used;
- when technology advances, the courts will be faced with the position that images over which there was no dispute as to their reliability cannot be received as evidence because they were not captured by technology which met the required specification; and
- the clear trend in the development of the law is to remove prior requirements for all forms of documentary evidence, leaving it to the courts to determine whether the evidence is in fact reliable.

3.17 For these reasons we are not convinced that some sort of criteria must be met before evidence can be admitted. Rather we agreed with the witnesses who said that there should not be different rules about admissibility based on the technology used to capture the evidence (eg IBM Q 306). There might be occasions where the most mundane home video could produce very useful evidence for the court which would be unlikely to be disputed. Neither would we wish to exclude the vast majority of business documents and other images in use today which may not meet some technical standard or other (cf Mr Smith Q 95, IBM p 99). Similarly, one can hardly expect those engaged in criminal activities to conform (Mr Sommer Q 118)!

3.18 **We recommend that evidence should not necessarily be inadmissible because it does not conform with some specific technological requirement.**

3.19 But, although we recommend that there should be no technological requirements which all digital images must meet before they can be admitted in evidence, this does not mean we are against authentication technologies. It is a matter for the courts to determine the evidential weight and reliability of an image, including the effects of any modification. We support the application of any technology which can help with the verification of an image and provide assistance to the courts in assessing the worth of the evidence before it.

3.20 **We recommend that the Government encourage the use of authentication techniques. Members of the legal profession should be made aware of the benefits of these**

techniques, their value in adding weight to evidence and the possible significance of their omission.

3.21 Technical procedures are only part of the authentication process or audit trail. In addition the provenance of evidence can be enhanced by procedural measures. Good practice for handling digital documents has been set down by the British Standards Institution[22] but conformance with this standard is perhaps not as widespread as it could be. Certainly it is good business practice to conform to such standards in preparing documents that might be used in court. **We recommend that the Government produce guidance on the benefits of conformance with procedural measures necessary to establish the reliability of evidence, with particular reference to existing standards. When this guidance is available, we recommend that the trade associations of those organisations likely to be concerned with it produce training material on its use.**

Identification in the Criminal Court

3.22 A real danger posed by digital image technology is that of misidentification, particularly in criminal prosecutions. The law is already alive to this danger and contains safeguards to ensure that undue weight is not given to identification evidence. In the 1960s a series of miscarriages of justice were caused by mistaken identification of defendants, and subsequently in the case of *R v. Turnbull*[23] the Court of Appeal (a full Court) laid down guidelines to be observed by judges when 'identity' is an issue. This has become known as the Turnbull Warning.

> "First, whenever the case against an accused depends wholly or substantially on the correctness of one or more identifications of the accused which the defence alleges to be mistaken, the judge should warn the jury of the special need for caution before convicting the accused in reliance on the correctness of the identification or identifications. In addition, he should instruct them as to the reason for the need for such a warning and should make some reference to the possibility that a mistaken witness can be a convincing one and that a number of such witnesses can all be mistaken ...
>
> Secondly, the judge should direct the jury to examine closely the circumstances in which the identification by each witness came to be made. How long did the witness have the accused under observation? At what distance? In what light? Was the observation impeded in any way, as for example, by passing traffic or a press of people? Had the witness ever seen the accused before? How often? If only occasionally, had he any special reason for remembering the accused? How long elapsed between the original observation and the subsequent identification to the police? Was there any material discrepancy between the description of the accused given to the police by the witness when first seen by them and his actual appearance? If in any case, whether it is being dealt with summarily or on indictment, the prosecution have reason to believe that there is such a material discrepancy they should supply the accused or his legal advisers with particulars of the description the police were first given ... Finally [the judge] should remind the jury of any specific weaknesses which had appeared in the identification evidence ...
>
> When, in the judgement of the trial judge, the quality of the identifying evidence is poor ... [he] should then withdraw the case from the jury and direct an acquittal unless there is other evidence which goes to support the correctness of the identification ..."

3.23 More recently, the Court of Appeal has recognised that similar dangers are posed by video evidence of identity:

---

[22] BSI DISC PD 0008, see footnote to paragraph 3.2.

[23] *R v. Turnbull* (1977) QB 224

> "some at least of the considerations underlying the safeguards built into the regulatory procedures laid down for identity parades and the showing of photographs come into play too with regard to the showing of video tapes. Particularly in cases where the quality of the video is poor or the opportunity it provides for recognition is limited ... it would be desirable to regulate its showing so as to maximise the prospects of any recognition evidence being truly spontaneous and independent and minimise the risk of anything being said or done which might infect that independence and spontaneity and instead prompt the recognition of some particular person ... It is not for this court to suggest what the appropriate procedures should be; clearly regard will need to be had to the practicalities. We would, however, urge that some immediate thought be given to this matter at a high level"[24].

3.24 In 1995, *R v. Clare and Peach*[25] demonstrated the ability of the law to adapt to video technology. The defendants were charged with offences of violence at a football match, the incident having been captured on an unclear, black-and-white video recording. A police officer compared this recording, frame by frame, with a high-quality, colour recording made of the crowd entering the stadium, and was thereby able to identify the defendants as having taken part in the violence. The Court of Appeal held that their conviction on this evidence was safe because an appropriate version of the Turnbull Warning was given to the jury. Lord Taylor said:

> "... as technology develops, evidential practice will need to be evolved to accommodate it. Whilst the Courts must be vigilant to ensure that no unfairness results, they should not block steps which enable the jury to gain full assistance from the technology"[26].

3.25 To date the courts have not developed a definitive statement of the safeguards which will be necessary where video evidence has been collected by a source other than a public body, or where image enhancement has been attempted as part of the identification process.

3.26 A further consideration arises in those cases which may be equally dependent on identification but where there is an image that unambiguously shows the defendant. It is not a matter of caution whether there can be a mistake in identifying the person whose image is submitted as evidence, of that there might be no doubt: it is a matter of caution over the probity of that evidence.

3.27 **We recommend that consideration be given to the Turnbull Warning being appropriately adapted so that the uncertainties inherent in images as evidence are made clear to the jury, particularly the implications of any measures to substantiate authenticity and breaks in the audit trail, and any processing which the image has undergone. This is a matter which the Judicial Studies Board may care to take up.**

The current need for greater certainty

3.28 It can be argued that existing law is likely always to be adequate and, where there is any uncertainty, this can be resolved by the courts in the normal process of building up case law. But allowing the precedents of case law to establish the legal requirements, is a lengthy and for the trailblazing litigant an expensive process. We noted a marked reluctance of both civil (Abbey National, QQ 324, 344) and criminal authorities (City of London Police) to be the first to become involved in litigation about digital images. If no cases are heard, no case law is developed—and uncertainty grows. With large investments hinging on the outcome, case law is not an ideal way of establishing the necessary legal confidence. A number of witnesses, including the Abbey National (QQ 375–379), the BSI (QQ 196–200) and Mr Sommer (Q 117) called for a code of practice or guidance for handling computer derived evidence: something "to give the managers confidence to take that leap and start to move away from this paper culture that we are now in" (Abbey National Q 376). The uncertainty must be resolved. The matter could be tested by a claim for a declaration in the High Court by means of a friendly action brought by a major institution; alternatively it could be the subject matter of consideration by the Commercial Court Users Committee; or the Government might consider issuing guidance, which of course would not be binding on the courts. **We recommend that consideration be given to these matters and the Government ensures there is a satisfactory resolution of the uncertainty.**

---

[24] *R v. Caldwell & Dixon* (1993) 99 Cr App. Rep. 73, 78 *per* Brown Wilkinson LJ.

[25] *R v. Clare and Peach* (1995) 2 Cr App. Rep. 333.

[26] (1995) 2 Cr App. Rep. 333, 339.

Maintaining confidence in the accuracy of the image

3.29 A danger frequently pointed out to the Committee was that of portraying image enhancement as an entirely objective science, particularly where an operator was manipulating the image to look for a suspect. It can become a largely subjective exercise. It might be possible, with certain software (eg the Home Office 'IMPROVE' software), to reproduce any changes, but this makes them no less subjective. Put at its simplest: if an operator is looking for a white car there is a temptation to increase the brightness of the image of a grey one; conversely when looking for a black car, the brightness is reduced (Liberty Q 5). This might occur without any malice. It is a simple desire to find what is being searched for: "the well intentioned mistake" that could lead to a miscarriage of justice (Mr Sommer Q 123). However we were told by the Home Office (p 127) that although the use of IMPROVE had been widespread since 1990, it had not been challenged as evidence.

3.30 Where the record has been altered, or the technology allows the possibility of alteration, the user will need to be able to prove that the image is authentic. Doubts will arise where there is a possibility that through human or machine error the record has become corrupted or confused with some other record[27]. Doubts will also be raised if fraud is suspected but, and this is an important point at the centre of many of our recommendations on awareness, the apparent credibility of an altered digital image may mean that fraud is not considered in the first place (eg Mr Sommer Q 140).

3.31 Furthermore, there is a danger that an altered image could be given an authenticating mark if the authentication were not done at the time of image capture. The value of such technologies would then be compromised. We also recognise that any authentication technology, however sophisticated, has the potential for being circumvented. Authenticating technologies will thus need to keep ahead of the abilities of those who set out to undo them. But these apparent shortcomings are possibly less real in practice than in theory. Our witness from IBM said of circumvention technologies: "in all of these processes the only thing that you can do is make it very difficult, and if you can make it difficult enough, such as that the process takes too long, then you are at least achieving part of your aim" (Q 292). We concluded that watermarks can be used to great advantage: they can provide a high level of security in conjunction with an audit trail and the cost of introducing a watermark to an image is likely to be low relative to the costs of trying to circumvent it. Of course the veracity of the witness presenting evidence should be considered alongside the evidence itself (QQ 99, 118).

3.32 What is important is to encourage the adoption of authentication technologies by creating a wide understanding of the benefits from the level of security they can provide. The technologies are advancing rapidly and there will also be the need to provide regular updates to both the users and suppliers on improvements and changes. The Government already gives 'type approval' for certain enforcement technologies using images as evidence and we see the measures set out above as an extension of this.

---

[27] Such doubts can be overcome by producing evidence as to the technical efficiency of the system, the maintenance of logs sufficient to indicate problems, error-checking procedures, management and training of staff, etc. Adherence to technical standards will assist in authentication, although even standards which are designed to achieve authentication cannot be guaranteed to do so, as English law has no system of certification which would raise a presumption of authenticity.

3.33 **We recommend that the Government encourages the adoption of technological measures for the authentication of images as evidence by giving type approval to them. The Forensic Science Service should provide ongoing advice for manufacturers and users of imaging equipment on authentication technologies.**

3.34 We noted in paragraph 3.6 that hitherto audit trails have not been demanded in cases where video images were used by the prosecution and in paragraph 3.11 we have made a recommendation on the need for greater public awareness of the particular circumstances relating to the need for paper originals. Overall we see a need for awareness by all those concerned with the potential difficulties with digital evidence. **We recommend that the Judicial Studies Board consider establishing a programme of education on the implications of digital technology for the judicial system.**

3.35 But if there is increased awareness, the defence may have insufficient financial resources to undertake technical investigations and to secure expert witnesses capable of challenging the reliability of an image. This is likely to be a particular problem where the defence is funded by legal aid. What is needed is some mechanism to make compliance with good practice, conformance with codes of management and the application of technological measures, accepted normal practice.

3.36 Voluntary standards and codes exist for the procedural measures necessary for document handling (eg the BSI code). We have recommended that similar codes and standards be put in place to encourage the use of technological measures to authenticate images. The advantage of such voluntary standards is that they can be changed to keep pace with changes in technology (or made substantially independent of it), they represent the consensus of those in the field and enable a far more flexible approach than is possible with regulation. But to achieve the full benefits from such codes there must be an incentive to comply with them. This is achieved in other areas by making compliance with an approved code a recognised way of showing that legal requirements have been met or that good practice has been achieved. **We recommend that the Government devise incentives or put in place measures such as the endorsement of relevant codes, to increase the adoption of good practice.**

CHAPTER 4 CIVIL LIBERTY IMPLICATIONS

4.1 Several witnesses drew our attention to the way surveillance systems in public spaces (sites to which the public has free access) intrude on individual privacy and civil rights. It was not our intention to examine these issues in detail. Any major consideration of proposed changes to the Data Protection Act and the implementation of the European Convention on Human Rights is clearly beyond our present remit. Nevertheless, we wish to see public acceptance and approval of the use of surveillance in public places maintained and encouraged. Systems which help to deter crime and assist the authorities to catch and prosecute criminals should be widely valued.

4.2 The potential for cost reduction offered by digital technology suggests that in future many CCTV surveillance systems will adopt this technique. With the technology comes the ability to alter images in the way that we have discussed in Chapter 3 and the potential ability to introduce data matching. Because we foresee an inevitable increase in the use of digitial surveillance systems we think it right to draw attention to the views of our witnesses who have commented on privacy and civil liberty factors.

City Centre Surveillance

4.3 Closed circuit television (CCTV) is used extensively in the United Kingdom. There is a significant commitment of public money. Mr Davies (p 31) estimated that between £150 million and £300 million is spent each year on surveillance equipment in the United Kingdom, and the Home Office has assisted in funding around 550 CCTV schemes over three 'challenge' competitions: distributing more than £37 million since 1995 (p 131). Individual schemes, for example the Chelmsford town centre system, which cost £0.5 million to set up and costs £160,000 *per annum* to run (The Chief Constable of Essex, Mr Burrow Q 407), represent substantial investment for a local authority. Many of our witnesses expect this scale of commitment to rise in the future.

Benefits and Concerns

4.4 CCTV undeniably provides the public with a sense of security. Shoppers in the city at night and motorists using public car parks feel safer, and experience that most basic of freedoms: the "right to move freely and safely in public places" (Symonds Group p 151). CCTV installations also form part of anti-terrorist measures, for example the system in the City of London, or help in the apprehension of criminals like the *Harrods* bombers or the murderers of Jamie Bulger. Surveillance plays a key part in crime prevention and Mr Burrow (Q 381) spoke about the reduction in recorded crime at particular locations. Many CCTV systems are used also on a day-to-day basis for controlling petty crime such as graffiti, littering and drunkenness.

4.5 It is less evident whether crime overall has reduced, or is merely relocated to areas outside the cover of surveillance systems. Notwithstanding the findings of some studies, for example in Airdie (Dr Norris, Q 36), data to support conclusions on the benefits of CCTV surveillance are weak. It was claimed that "less than 0.02 per cent" (Q 36) of the public money spent in this area was spent on evaluation. "Only four, maybe five, properly conducted evaluations by people who are statistically trained and criminologically aware as to the impact of CCTV" (Q 36) have been made. There was too often fundamental confusion between correlation and causation. The Chief Constable of Essex thought that "we ought to try harder [to obtain data on cost effectiveness] rather than just [rely on] the anecdotal evidence that we currently have"(Q 407).

4.6 We were encouraged by the Home Office response to our questions on the assessment of the effectiveness of CCTV systems in reducing crime and disorder (Mr Childs Q 454). Evaluation, we were told, now features more prominently in recent appraisals of schemes. While this is encouraging, the public need to be assured that good value for money is obtained. Given the large and continuing commitment of public resources **we recommend that the Government commission a substantial, rigorous and independent study of the cost and effectiveness of publicly funded surveillance systems.**

4.7 As already noted, concerns were raised about crime displacement and the use of surveillance systems to deal with public order offences. We share the sentiment behind the statement of Mr Leach (Q 37) that "we simply do not believe that there is enough adequate evidence to enable us to be sure about the extent to which crime has been reduced". Such information would be of great benefit in reaching decisions about future investment in surveillance systems. As the collection of the data necessary for the thorough study we are recommending may take some time, **we further recommend that an interim report be available within 12 months to provide a broad indication of the scale of any increase in convictions, any reductions in crime and the fear of crime, and separately disorder, that has been achieved by public space surveillance systems.**

4.8 We were told of a MORI poll taken in Colchester (Q 381) where 52 per cent of respondents said that the city centre system made them feel safer. No one felt that it made them feel less safe. More surprising was Dr Norris' account (Q 43) of work done at the Scottish Centre for Criminology. This showed that if the questions about acceptability are rephrased from concerns about the fear of crime to concerns about civil liberties then the level of support for CCTV appears to decline dramatically, in the case reported from around 90 per cent to about 50 per cent. The LGIU quoted (p 58) a 1992 Home Office report (*Closed Circuit Television in Public Places*, Crime Prevention Unit Paper 35) which concluded: "public acceptance is based on limited, and partly inaccurate knowledge of the functions and capabilities of CCTV systems in public places". Mr Burrow reported (Q 393) that he did not think the public were aware of the capabilities and the degree of control over CCTV. He stated "there is public confidence in the use of CCTV, but I feel that the confidence is fragile, and could be reversed" (Q 380). He believes that when public ignorance of the capabilities and intrusions of CCTV is replaced by awareness, then it "may well be that there will be a falling off of public confidence in the authorities having control of such systems" (Q 420). The research done at the Scottish Centre for Criminology reported by Dr Norris (Q 43) suggests that as the public acquire a greater understanding of the technology, support for CCTV (without which further investment and use could be severely curtailed) may decline. However extreme such views may be, the technology clearly has implications for privacy and civil liberties. Without sensitive handling these worries could override the deterrent and security enhancing benefits which derive from surveillance.

Current Controls over the use of CCTV

4.9 There are no statutory, or other, controls on the use of public space CCTV systems. The police are subject to 1984 Home Office Guidelines relating to the use of equipment in surveillance operations generally. These require, for example, that a Chief Superintendent satisfy himself that the use of CCTV equipment "will not involve any unwarrantable intrusion of privacy" (p 130). There are more stringent requirements relating to intrusive surveillance, but guidelines do not provide any enforceable rights to individuals. Any public space surveillance scheme has to have a code of practice in place before it will receive Home Office funding and, although the Home Office endorses the LGIU code (see Box 5), local practice may differ. Moreover, these codes are not enforceable in the courts. They have even less application to private systems. We were told by the Home Office that there is no reliable information on the use of the LGIU code by privately owned and operated schemes (p 130). The Data Protection Act 1984 applies only to systems that are capable of automatically processing personal data by reference to an individual. At present most systems do not appear to meet the criteria of the 1984 Act. So it does not apply. We found no evidence that this lack of regulation is widely appreciated by the public (Mr Burrow Q 393).

Control of public CCTV Images

4.10 A number of our witnesses expressed concern over the way images from surveillance systems were being released into the public domain (eg pp 14, 58, 116). Some police forces, for example City of London Police and Greater Manchester Police stated that they would not release images to anyone except other police or Customs and Excise authorities making investigations into crime, unless they were required to do so by court order. Our impression is that some other Forces have different policies and extracts from tapes shown on television suggest a more relaxed attitude

Box 5: "A Watching Brief"

Summary of main points of the *Local Government Information Unit Code of Practice for CCTV*. This is a voluntary code of practice. Where the Code is being used it is often adapted by operators for their own purposes and not all of the following points will apply.

Start-up

- The purpose and objectives of the scheme must be clearly identified, based on local needs. An 'owner' must be identified for the purposes of accountability. If the scheme is a partnership then all partners must agree the code and any changes to it or to the system,
- It must be established whether the activities fall within the scope of the Data Protection Act 1984 and, if so, registration with the Registrar is required.
- Consultation must be held with the public, tenants and residents, trade and other local groups *prior* to installation and for regular evaluation of the scheme. (Discussion to include purpose of scheme, coverage, camera locations, effectiveness). Further consultation must be held if significant changes to the system are considered.

System requirements

- Installation of equipment must be carried out in consultation with the police.
- No sound should be recorded in public spaces. Dummy cameras should not be used. Cameras should not be hidden. Cameras should be restrained so that they do not look into private property.

Control room

- Staff must sign a confidentiality agreement and attend training on privacy issues.
- Individuals should not be targeted without good reason.
- The control room must be secure. Access to monitors should be restricted to authorised staff. Records of access should be kept. Public access must not be allowed except for "lawful, proper and sufficient reasons".

Tapes

- The owner should produce a statement of intent on the use and access to recorded material. Recorded material must not be sold or used for commercial purposes.
- Recording equipment should be checked daily and tested monthly. Tapes must be maintained, erased before use, retained for a maximum of 31 days, and be stored and disposed of securely. All tapes should be catalogued. Any tape to be used for evidential purposes must be stored separately and securely.
- Access to tapes may be obtained through court order and by lawyers acting for defendants or crime victims. No other access will be allowed unless it is for reasons which fall within the purposes and objective of the scheme.

On-going compliance

- The owner of the scheme has ultimate responsibility for management of the system, implementing the code, and protecting public and individual interests. The owner must provide information to the public about the scheme (including the complaints procedure).
- The local authority should receive an annual report on the scheme. This and the code of practice must be made available to the public. There should be regular evaluation of the scheme and its effectiveness. There should be a regular audit of the scheme and code of practice compliance by a senior person and by an independent group.
- Information should be exchanged with the police (eg on code compliance). If the police are sole operators, then compliance should be monitored by the police authority.

than that taken by the City of London Police. The reasons why the authorities originally installed their surveillance systems may account for some of the differences in their rules. But there is no broad overall policy even though the LGIU code is quite clear: "recorded material must only be used for the purposes defined in the code ... In particular recorded material will not be sold or used for commercial purposes or the provision of entertainment" (Box 5).

4.11 During the course of our Enquiry the 'Peck case' came before the Court of Appeal. Mr Peck was captured on a CCTV system in Brentwood attempting to commit suicide. He was in the road with a knife attempting to slash his wrists. The Police were alerted and the tape showed the two police officers arriving. They approached the man with the knife, took hold of him and then, realising that he was suffering from some mental disorder and was attempting to commit suicide, sent him to hospital. Brentwood Council subsequently released the video to the BBC. Mr Peck sought a judicial review in the High Court but the Court found there was no breach of the law. We also learnt that police authorities might be receiving payment from the media for tapes used in a variety of TV programmes. There may be very acceptable and beneficial reasons for getting the media to publish such material, for example to help the police in tracing suspects. But we perceive the potential of serious damage to public confidence if the use of CCTV systems were to become associated primarily with the provision of entertainment, even if of educational value. There are a number of conflicting and sensitive issues here which merit study. **We recommend that the Government establish a uniform policy on the control and release of CCTV derived images from publicly owned surveillance systems.** Considerations should then be given to the application of a similar policy to privately owned systems.

Surveillance Coverage

4.12 The widespread use of surveillance equipment, both publicly and privately operated, raises difficult issues of informing the individuals who may be observed by these systems. The present principle as endorsed in the LGIU voluntary code, is that all such systems should have prominently displayed notices to make members of the public aware that their image is being recorded and by whom. While many such notices do exist, large city centres deploy numerous cameras to cover a wide area. For example, around the Palace of Westminster it is possible to view individuals on the far side of Westminster Bridge, at the end of Whitehall and in Victoria Tower Gardens off Millbank from one control-room position, and at the same time, by day or night. It is unrealistic to expect those who install and operate such wide coverage systems to post notices at every street corner for the public to read. At many other locations where the scale of coverage is much less extensive, it will be feasible and sensible to provide notices.

Control of CCTV in spaces to which the public has free access

4.13 It is frequently difficult for members of the public to determine the exact boundary between public and private property. We do not think the legal boundary matters. Walking from the street into a shopping mall, then into a large store and thence into a small boutique within that store, the shopper may cross many boundaries of legal ownership. Because the public can distinguish no difference between the various CCTV systems any breach of public trust by a private operator will result in a loss of confidence in the public system also.

4.14 We found a broad spectrum of support for improved control of public space surveillance schemes. Evidence from groups such as Justice and Liberty together with other concerned individuals (pp 1, 10, 31) called for increased control. Organisations such as the Law Society of Scotland stated that "there should be statutory controls on the placement and use of surveillance cameras and the release of information from them" (p 156). The surveillance industry added their own call for stricter control. Symonds Group said that "we believe strict statutory controls should be introduced to govern [CCTV] placement, use, and access to the consequential information". We particularly draw attention to the evidence from the Association of Chief Police Officers (p 116) that "the Police Service would ... encourage legislation regulating surveillance technology and governing the unauthorised disclosure of information so obtained". We believe that public confidence in the future use of CCTV surveillance as it is more widely deployed in the fight against crime and disorder is at issue. **We recommend that the Government give urgent consideration to introducing tighter control over any system, either publicly or privately owned, covering sites to which the public has free access. To meet the requirement for continued public support, we would expect this to cover, but not exclusively, the need for some form of licensing; for statutory or other enforceable codes of practice; and for powers to inspect and audit the use and handling of surveillance systems, including the images, their storage and disposal.**

The Data Protection Act

4.15 A fundamental principle behind the Data Protection Act 1984 is that material should be collected for specified and legitimate purposes, and used and disclosed only in ways compatible with those purposes. Yet, as already noted, the Act only applies to CCTV material in the relatively rare circumstance that the data were recorded and processed with respect to an individual.

4.16 In both written and oral evidence from the Data Protection Registrar (QQ 222–259, p 76) we were struck by the commonality of purpose behind her remit and the objectives which we believe should be applied to the control of CCTV. We share the view that "it is not so much the existence of technology that poses a threat to the civil liberties of the individual, but the use that is made of the technology and the setting in which surveillance takes place" (p 79). The principles of the Act, on the relevance of information, fair processing and disclosure, are just those which should be applied to public space surveillance.

4.17 As we complete our report a new Data Protection Bill has been introduced in Parliament[28]. **We would like to see the new law encompass CCTV and the DPR be given responsibility to issue or oversee enforceable codes of practice for such systems. The maintenance of public support for CCTV would be further strengthened if the DPR were to be given powers to check, that is to audit, the operation of these systems, and not to have to wait for a complaint to be lodged before taking action.**

Data matching

4.18 The Government is looking at the provision of electronic services and these are measures we firmly support. Data matching is a particular concern for this Enquiry where image recognition techniques are used (see Box 6). In the City of London we saw a number plate matching system in operation and we were impressed by the speed with which it could process vehicle information. The Symonds Group held the view that: "if cameras are used in conjunction with image tracking software then the effectiveness of surveillance is vastly improved and thus the implications of civil liberties are increased" (p 151). If the technology continues to develop as expected it may in the future be possible to match data from the digitised passport photographs that are coming into use (p 127) with other databases, enabling the rapid identification of individuals who were, for example, attending a football match. This might cause justifiable unease. It is clear that image recognition technologies have an important role to play in assuring security, but controls on their use may be needed to strike a fair balance with civil liberties.

4.19 Although we did not take evidence and did not consider all of the issues of image recognition and data matching in detail, it is an area where the technology is pressing ahead and the public debate lagging far behind. It is possible that there will be disquiet over the implications of data-matching in general and image recognition in particular. We were therefore surprised that there was no published guidance for Government Departments on data-matching and related technologies (p 171).

---

[28] The Data Protection Bill, HL Bill 61, 14 January 1998

Box 6: Image recognition

Most cameras are passive, unintelligent devices which take a picture and leave the processing and interpretation to human operators. If a computer is linked to an image input device (either a camera or a scanner) it is possible to automate some of the interpretation, to speed up the interpretation process dramatically and to cross-match the image to other databases. There are numerous applications of this technology but three have, perhaps, the widest implications for images used as evidence: character recognition from scanned documents, number plate recognition (from images taken by surveillance or enforcement cameras), and face recognition.

Character recognition

Character recognition software is often used in conjunction with document scanners to convert the image into a word processing file. The document is scanned to produce a digital image and then the recognition software interprets areas of text within the image, translating data patterns into appropriate text files. There are a number of advantages over the original scanned image: the new file uses considerably less memory; the document can be treated as any other word processing file, rather than as an image; the quality of the document as displayed on screen is often greatly improved; and the document becomes searchable using standard techniques.

Number plate recognition

This was demonstrated to the Committee by the City of London Police who use a system of cameras to monitor vehicular access to and from a controlled zone within the City. The principle is similar to character recognition discussed above. A camera films the vehicles, software interprets which section of the image is the number plate, and then character recognition software interprets the picture elements to make a 'best guess' of the numbers and letters in the number plate. In the City of London operation the system processes around 114,000 vehicles a day. It takes about four seconds to identify not only the number plate, but also to cross-check it with local Police databases and the Police National Computer and then alert the control centre operators if there is a match (eg if the vehicle has been registered as stolen). The recognition software does make errors and so the video still image of any number plate which is difficult to identify (eg obscured by mud), and any number plate which is flagged for further attention because it cross-matches with a database entry, is displayed in the control room alongside the interpretation for human verification.

Face recognition

Face recognition is still in the development stages because of the scale of complexity involved. As well as needing to define what makes faces different enough for a computer to distinguish individuals, a reliable system would have to overcome differences in facial expression, head angle, lighting, movement, and ephemeral features such as sun tans, hair style, facial hair, make-up, hats and sunglasses too! A comparative database of faces identified with individuals is a prerequisite, and such a database may need to contain multiple images of each person: a database of this kind does not exist, and there might be intense opposition if it were attempted to create one.

4.20 **We recommend the Government produces guidance for both the public and private sectors on the use of data matching, and in particular the linking of surveillance systems with other databases.**

4.21 Individuals may not be aware of the existence of information on them derived by reference to two or more unrelated databases. They will therefore not recognise if there is a need to approach the DPR who can act only if a complaint has been made. **We recommend that the DPR be given powers to audit the operation of datamatching systems.**

Conclusion

4.22 Any form of surveillance is also a form of intrusion. The question to be considered is whether such intrusion can be justified (p 151). In this chapter we sought ways to harmonise the interests involved. An individual's right to privacy and the interest of both the individual and society in the prevention of crime and disorder need to be fairly balanced. Essential and unavoidable compromises must be widely appreciated. Our recommendations for a degree of greater control over the installation, use and release of images from public space surveillance systems seek to chart a way to achieve that balance. **We want to see public acceptance of surveillance, introduced to deter and assist in the capture and prosecution of criminals, blossom and flourish. This is more likely to be the case if there is wide public debate of the issues involved, and we recommend that the Government should promote such debate.**

CHAPTER 5 SUMMARY AND RECOMMENDATIONS

5.1 We were pleased to find that Digital Images, which we initially thought might create difficulties for the courts, do not.

5.2 But many people think there will be difficulty in obtaining legal acceptance of digital images. And many who understand there is no legal problem fail to appreciate fully the potential for tampering that the technology creates. The perceived difficulties mean that opportunities are missed—a reluctance to use digital imaging technology or to dispose of paper records, for example—and the failure to understand fully the process means that too great a reliance can be placed on photographic or video evidence. The doubts and scepticism normally associated with unsubstantiated pieces of paper may be suspended when confronted with a very believable picture.

5.3 To counter the common misconception about the need for original documents, **we recommend that the Government encourage the appropriate legal bodies to draw greater attention to the change to digital document processing and to widen public awareness that paper originals are rarely necessary.** (Paragraph 3.11)

5.4 We do not support moves to establish specific requirements before digital images can be used as evidence and **we recommend that evidence should not necessarily be inadmissible because it does not conform with some specific technological requirement.** (Paragraph 3.18)

5.5 But we are in favour of technical measures that assist with authentication of images and **we recommend that the Government encourage the use of authentication techniques. Members of the legal profession should be made aware of the benefits of these techniques, their value in adding weight to evidence and the possible significance of their omission.** (Paragraph 3.20). Further, **we recommend that the Government encourages the adoption of technological measures for the authentication of images as evidence by giving type approval to them. The Forensic Science Service should provide ongoing advice for manufacturers and users of imaging equipment on authentication technologies.** (Paragraph 3.33)

5.6 We were impressed by the work that has already been undertaken in setting standards for handling digital documents. **We recommend the Government produces guidance on the benefits of conformance with procedural measures necessary to establish the reliability of evidence, with particular reference to existing standards. When this guidance is available, we recommend that the trade associations of those organisations likely to be concerned with it produce training material on its use.** (Paragraph 3.21)

5.7 We were shown examples of processed images and the capability of programmes designed to manipulate photographs. They provide believable images that are still very convincing even when the changes are explained and well understood. We think this technology raises the possibility that people who are not familiar with it can be too easily misled. **We recommend that consideration be given to the Turnbull Warning being appropriately adapted so that the uncertainties inherent in images as evidence are made clear to the jury, particularly the implications of any measures to substantiate authenticity and breaks in the audit trail, and any processing which the image has undergone. This is a matter the Judicial Studies Board may care to take up.** (Paragraph 3.27)

5.8 The normal development of case law is too slow a process to generate the required degree of legal confidence in time to keep pace with developments in digital imaging technology. **We recommend that consideration be given to measures to reduce the uncertainty over the use of digital images in court and Government ensures that there is a satisfactory resolution of the uncertainty.** (Paragraph 3.28)

5.9 To help improve the awareness of the potential difficulties with digital evidence and to encourage the adoption of good practice in the preparation of material for the courts **we**

recommend that Government devise incentives or put in place measures such as the endorsement of relevant codes to increase the adoption of good practice. (Paragraph 3.36)

5.10 Overall we see a need for awareness by all those who are concerned with the potential difficulties with digital evidence. **We recommend that the Judicial Studies Board consider establishing a programme of education on the implications of digital technologies for the judicial system.** (Paragraph 3.34)

5.11 Although not a major feature of our enquiry our examination of the use of CCTV left us with concerns that what seems to be a very valuable technology for crime prevention and the maintenance of law and order could be in danger of losing public confidence through the perception of improper use. But although we were convinced that it was a valuable tool of law enforcement we were not convinced that sufficient data exist to support the overall level of expenditure. **We recommend that the Government commission a substantial, rigorous and independent study of the cost and effectiveness of publicly funded surveillance systems.** (Paragraph 4.6) **We further recommend that an interim report be available within 12 months to provide a broad indication of the scale of any increase in convictions, any reductions in crime and the fear of crime, and separately, disorder, that has been achieved by public space surveillance systems.** (Paragraph 4.7)

5.12 One particular practice that we felt was very likely to endanger public acceptance of surveillance schemes was the use of material so obtained for entertainment purposes, however apparently well justified it might be as training or educational material. **We recommend that the Government establish a uniform policy on the control and release of CCTV derived images from publicly owned surveillance systems.** (Paragraph 4.11)

5.13 We concluded that to maintain public confidence in the use of CCTV surveillance technology for the prevention of crime and disorder greater control of its use was needed. **We recommend that the Government give urgent consideration to introducing tighter control over any system, either publicly or privately owned, covering sites to which the public has free access. To meet the requirement for continued public support, we would expect this to cover, but not exclusively, the need for some form of licensing; for statutory or other enforceable codes of practice; and for powers to inspect and audit the use and handling of surveillance systems, including the images, their storage and disposal.** (Paragraph 4.14)

5.14 Data matching technology is advancing rapidly and although we felt some concerns could be overstated we can see difficulties if insufficient attention is paid to potential problems. **We recommend that the Government produces guidance for both the public and private sectors on the use of data matching, and in particular the linking of surveillance systems with other databases.** (Paragraph 4.20)

5.15 We have not made a specific legislative proposal for improved control over public space CCTV systems but the similarity of our objectives with the current Data Protection Act suggest this, or its successor, might be an appropriate vehicle. **We would like to see the new law encompass CCTV and the DPR be given responsibility to issue or oversee enforceable codes of practice for such systems. The maintenance of public support for CCTV would be further strengthened if the DPR were to be given powers to check, that is to audit, the operation of these systems, and not to have to wait for a complaint to be lodged before taking action.** (Paragraph 4.17). **The DPR should also be given powers to audit the operation of datamatching systems.** (Paragraph 4.21)

5.16 Our recommendations for a degree of greater control over the installation, use and release of images from public space surveillance systems seek to chart a way to achieve that balance. **We want to see public acceptance of surveillance, introduced to deter and assist in the capture and prosecution of criminals, blossom and flourish. This is more likely to be the case if there is wide public debate of the issues involved, and we recommend that the Government should promote such debate.** (Paragraph 4.22)

APPENDIX 1

Sub-Committee II: Digital Images as Evidence

The members of Sub-Committee II were:

L. Ackner
L. Brain
L. Carmichael of Kelvingrove
L. Craig of Radley (Chairman)
L. Flowers
B. Hogg
L. Howie of Troon
L. Kirkwood
Bp. of Leicester
L. Nathan
L. Tombs

The Sub-Committee appointed as its Specialist Adviser Mr Chris Reed, Reader in Information Technology Law at Queen Mary and Westfield College.

APPENDIX 2

Call for Evidence

The House of Lords Science and Technology Committee has appointed Sub-Committee II, under the chairmanship of Lord Craig of Radley, to conduct an enquiry into the use of digital images as evidence.

Because digital images are easy to copy and it may be difficult to distinguish a copy, or a copy which has been "doctored", from the original, concern has been raised over their use as evidence. As analogue systems are being displaced by digital ones and the investment in digital technology for image capture and signal processing increases, it is important that any concerns over the use of this technology be addressed now if wise investment decisions are to be made.

The enquiry will examine the need for any special measures to ensure the integrity and authenticity of digital images. It will consider if any measures are necessary to ensure that modern image processing technologies, such as compression and enhancement techniques when applied to either digital or analogue images, are acceptable in court. It will also examine the implications of video surveillance technologies for civil liberties.

The Sub-Committee invites written submissions on all matters relevant to this topic, but in particular on the questions listed below, with a view to making a report to the House of Lords early in 1998.

1. What is the current and forecast future use of digital technology for image collection, storage and transmission? What is its use by the courts and the legal profession? What is the state of the art of image manipulation?

2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?

3. Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?

4. Under what circumstances and with what controls should modified or enhanced images be used as evidence?

5. Do technologies which compress data or use error correction technology when transmitting it raise special problems ?

6. Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?

7. Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?

8. Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?

9. Is there the need for special measures to control the publication of modified images by the media?

APPENDIX 3

List of Witnesses

Those marked * gave oral evidence.

* Abbey National plc
* Association of Chief Police Officers
Association of Chief Police Officers (Scotland)
AEA Technology
* Baker & McKenzie
* Bird & Bird
* British Standards Institution
Broadcasting Standards Commission
CITU, Cabinet Office
Chartered Institute of Arbitrators
Computer and Systems Telecommunications Ltd
Crown Prosecution Service
* Data Protection Registrar
* Mr Simon Davies, Privacy International
Faculty of Advocates
Defence Evaluation and Research Agency, Ministry of Defence
General Council of the Bar
* Home Office
* IBM United Kingdom Ltd
Information Security Bulletin
* Justice
Law Society of Scotland
* Liberty
* Local Government Information Unit
Mr Grady Miller, Trade Policy Analyst
Press Complaints Commission
Royal Photographic Society
Screen plc
Security Facilities Executive
* Mr Peter Sommer (London School of Economics)
* Mr Alan Shipman
Symonds Group Ltd
University of Stirling

APPENDIX 4

Acronyms

ACPO	Association of Chief Police Officers
BSI	British Standards Institution
CCD	Charge Coupled Device
CCTV	Closed Circuit Television
CDROM	Compact Disc Read Only Memory
CITU	Office of Public Service Central IT Unit
CPS	Crown Prosecution Service
DPA	Data Protection Act (1984)
DPR	Data Protection Registrar
FSS	Forensic Science Service
LGIU	Local Government Information Unit
PACE	Police and Criminal Evidence Act (1984)
PSDB	Home Office Police Scientific Development Branch
WORM	Write Once Read Many (times)

Printed in the United Kingdom by The Stationery Office Limited
2/98 347402 19585

ISBN 0-10-406498-6

9 780104 064986

Published by The Stationery Office Limited
and available from:

The Publications Centre
(Mail, telephone and fax orders only)
PO Box 276, London SW8 5DT
General enquiries *Lo-call* 0345 023474
Telephone orders *Lo-call* 0345 585463
Fax orders 0171 873 8200

The Stationery Office Bookshops
59–60 Holborn Viaduct, London EC1A 2FD
(Temporary location until mid-1998)
Fax 0171 831 1326
68–69 Bull Street, Birmingham B4 6AD
0121 236 9696 Fax 0121 236 9699
33 Wine Street, Bristol BS1 2BQ
0117 9264306 Fax 0117 9294515
9–21 Princess Street, Manchester M60 8AS
0161 834 7201 Fax 0161 833 0634
16 Arthur Street, Belfast BT1 4GD
01232 238451 Fax 01232 235401
The Stationery Office Oriel Bookshop
The Friary, Cardiff CF1 4AA
01222 395548 Fax 01222 384347
71 Lothian Road, Edinburgh EH3 9AZ
(counter service only)

In addition customers in Scotland may mail,
telephone or fax their orders to:
Scottish Publication Sales,
South Gyle Crescent, Edinburgh EH12 9EB
0131 479 3141 Fax 0131 479 3142

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders 0171 219 3890
General enquiries 0171 219 3890
Fax orders 0171 219 3866

Accredited Agents
(see Yellow Pages)

and through good booksellers

©Parliamentary copyright House of Lords 1998
Applications for reproduction should be made in writing to the Copyright Unit,
Her Majesty's Stationery Office, St. Clements House, 2-16 Colegate, Norwich, NR3 1BQ
– Fax 01603 723000
ISBN 0 10 406498 6